ATTACHMENT 8

Reference F
Data Destruction Information and References

State of Alaska
Department of Health & Social Services

This is an overview of the State of Alaska and Federal Sources on data destruction requirements for confidential information. The department regards confidential information, information that identifies or could identify an individual) as personally identifiable information (PII).

Personally Identifiable Information (PII) and a subset of PII information the State of Alaska Department of Health & Social Services is responsible for as an Information Owner.

PII includes information on an individual such as the individual's name and includes one other identifier such as, a social security number, date of birth, driver's license number, account number, password, employee id, or other access codes.

There are many laws and regulations defining PII. Here are some examples:

- Alaska Personal Information Protection Act (APIPA)
- HIPAA\HITECH - Electronic Health Protected Information (ePHI)
- Payment Card Industry (PCI)
- Federal Tax Information (FTI)
- Criminal Justice Information (CJIS)

To meet the required compliance standards with PII (APIPA, ePHI, FTI, CJIS, etc) must be “purged” via some **physical means** rather than simply overwritten/deleted.

Alaska Statute AS 45.48, (APIPA), Section 45.48.500 -.590 concerns the Disposal of Records.

- This article contains provisions that require a business and a government agency to take reasonable measures to protect against unauthorized access to, or use of, records when disposing of records containing personal information. To comply with this requirement, a business or government agency can implement compliance and monitoring policies that require the destruction of personal information, or enter a contract with a third party for the disposal and destruction of the records. A business or government agency is not liable for the disposal after relinquishing control of the records to a third party that is in the business of record destruction.

Disposing of Information on Electronic Media

Approved guidelines for disposing of information on fixed and removable media containing Personally Identifiable Information (PII),

The contract may include additional language stipulating how PII is disposed of or destroyed upon the termination of the contract based on the PII subset type/data classification.

NIST SP 800-88, Guidelines for Media Sanitization

- Sanitization is a process to render access to target data (the data subject to the sanitization technique) on the media infeasible for a given level of recovery effort. The level of effort applied when attempting to retrieve data may range widely. For example, a party may attempt simple keyboard attacks without the use of specialized tools, skills, or knowledge of the media characteristics. On the other end of the spectrum, a party may have extensive capabilities and be able to apply state of the art laboratory techniques. *Clear, Purge, and Destroy* are actions that can be taken to sanitize media. The categories of sanitization are defined as follows:
    - *Clear* applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).
    - *Purge* applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques.
    - *Destroy* renders Target Data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data.

In the HIPAA Disposal FAQ it is indicates that PHI must be sanitized and references:

- For PHI on electronic media, clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating, or shredding).

HHS HIPAA Security Series 3: Security Standards – Physical Safeguards with the following criteria for reuse

- Are procedures developed and implemented for removal of EPHI from electronic media before re-use?
- Do the procedures specify situations when all EPHI must be permanently deleted or situations when the electronic media should only be reformatted so that no files are accessible?